Evaluation Report

OIG-CA-06-008

INFORMATION TECHNOLOGY: 2006 Evaluation of Treasury's FISMA Implementation

September 29, 2006

Office of
Inspector General

DEPARTMENT OF THE TREASURY

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

September 29, 2006

MEMORANDUM FOR IRA L. HOBBS
CHIEF INFORMATION OFFICER

FROM: Louis C. King
Acting Deputy Assistant Inspector General for Financial Management and Information Technology Audits

SUBJECT: 2006 Evaluation of Treasury's Federal Information Security Management Act Implementation

I am pleased to transmit the following reports:

- INFORMATION TECHNOLOGY: Evaluation of Federal Information Security Management Act Implementation for the FISMA Year 2006
- Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2006
- INFORMATION TECHNOLOGY: Fiscal Year 2006 Evaluation of Treasury's FISMA Implementation for Its Non-Intelligence National Security Systems [LIMITED OFFICIAL USE]
- INFORMATION TECHNOLOGY: Additional Actions Needed for System Inventory

The Federal Information Security Management Act of 2002 (FISMA) requires an annual independent evaluation of Treasury's information security program and practices. To meet FISMA requirements, we contracted with KPMG LLP, an independent certified public accounting firm, to perform the FISMA evaluation of Treasury's unclassified systems (Attachment 1), except for those of the Internal Revenue Service (IRS). The Treasury Inspector General for Tax Administration (TIGTA) performed the FISMA evaluation for the IRS systems[1] (Attachment 2). In addition, we performed the FISMA evaluations for non-intelligence national security systems (Attachment 3) and for intelligence program systems.[2]

[1] We did not review the work performed by TIGTA to evaluate the information security program and practices of the IRS. Our overall conclusions, insofar as they relate to the IRS, are based solely on TIGTA's report (Attachment 2). We did, however, coordinate with TIGTA on the scope and methodology (including sample selection) of our respective evaluations.

[2] The results of the evaluation for intelligence program systems are contained in Report No. OIG-CA-06-004. This report is classified.

We considered the results of the evaluations performed by KPMG LLP and TIGTA, as well as our own evaluations on national security systems, in assessing Treasury's overall compliance with FISMA. Based on the results of these evaluations, we believe that despite notable progress, Treasury has deficiencies that, in the aggregate, constitute substantial noncompliance with FISMA. The most important of these deficiencies follow:

- Non-IRS bureaus and offices within Treasury have significant deficiencies in their information security program and practices. KPMG LLP reported concerns in the following areas at various bureaus: certification and accreditation, training, plans of actions and milestones, system interfaces, security self-assessments, system categorization, configuration management process, and incident response process.
- IRS also continues to have shortcomings in its information security program and practices. TIGTA reported significant deficiencies in the following areas: continuous monitoring of systems, incident reporting procedures, and training employees with key security responsibilities.
- We reported several matters pertaining to national security systems.

We also identified areas where Treasury improved its information security program and practices. Most notably, Treasury improved its FISMA system inventory. During this FISMA reporting period, Treasury issued two memorandums defining the Treasury system inventory and providing instructions to bureaus on what information to collect to develop the inventory. In addition, representatives of the Office of the Chief Information Officer (OCIO) met with a number of bureaus to specifically address inventory issues. As a result of these and individual bureau efforts, Treasury now has complete and properly categorized inventories of its national security systems. We also generally agree with the OCIO on the total number of Treasury systems. However, as noted in Attachment 4, additional actions are needed to further improve the system inventory.

In addition, TIGTA reported that IRS has made steady progress in complying with FISMA requirements. TIGTA reported the IRS inventory is substantially complete and the risk categorizations for its systems are accurate. The IRS also made significant improvements in its security certification and accreditation process.

If you have any questions or require further information, please contact me at (202) 927-5774.

Attachments

ATTACHMENT 1

Information Technology: Evaluation of the Federal Information Security Management Act Implementation for FISMA Year 2006

Evaluation Report

For the

Department of the Treasury

Information Technology: Evaluation of Federal Information Security Management Act Implementation for the FISMA Year 2006

September 29, 2006

Prepared by:
KPMG LLP
2001 M Street, N.W.
Washington, D.C. 20036

UNITED STATES DEPARTMENT OF THE TREASURY
FISMA Year 2006 FISMA EVALUATION

Evaluation Report

Table of Contents

October 1, 2006

Louis C. King
Director, Information Technology Audits
Department of the Treasury, Office of Inspector General

To assist Federal agencies in meeting their responsibilities, the President signed into law on December 17, 2002, the Electronic Government Act. Title III of this Act, the Federal Information Security Management Act (FISMA), along with Office of Management & Budget's (OMB) policy, lays out a framework for annual Information Technology (IT) security reviews, reporting, and remediation planning. As required by FISMA, an annual independent evaluation was performed for the Department of the Treasury's (Treasury) information security program and practices to determine the effectiveness of such program and practices for FISMA Year (FY) 2006 as they relate to the 13 bureaus and Offices listed in Appendix A. FISMA requires the Inspector General or an independent external auditor, as determined by the Inspector General, to perform this evaluation. Treasury has two Inspectors General: The Treasury Inspector General for Tax Administration (TIGTA) (which covers the Internal Revenue Service (IRS)) and the Treasury Office of Inspector General (OIG) (which covers the remainder of Treasury).

For FY 2006, the OIG awarded a contract to KPMG LLP to perform the FISMA evaluation for Treasury's unclassified systems. The Treasury OIG performed the evaluation of national security systems, and the TIGTA performed the FISMA evaluation for the IRS.

Our objective, scope, and methodology are described in Appendix C. This report contains the results in brief, background, and responses to OMB questions, which contain the detailed results of our evaluation.

Results in Brief

Treasury's information security program and practices, as they relate to non-national security systems[1], require additional improvements to adequately protect the information and systems that support Treasury operations.

Provided below are specific areas where needed improvements were identified during the evaluation:

- Treasury's security certification and accreditation (C&A) process needs enhancement. The Department has not consistently developed C&A packages in accordance with guidance prescribed by the National Institute of Standards and Technology (NIST) Special Publications (SP) series as noted in the following examples:

[1] The evaluation of Treasury's information security program and practices for its national security systems is reported separately.

- Required components of the C&A packages have not been documented or are missing key elements.
- Child systems have not been documented in the C&A documentation of their parent systems.

We noted the above issues at the following Treasury bureaus[2]:

- Alcohol and Tobacco Trade and Tax Bureau (TTB)
- Community Development Financial Institution (CDFI) Fund
- U.S. Mint (Mint)
- Bureau of Engraving and Printing (BEP)
- Office of the Comptroller of the Currency (OCC)
- Departmental Offices (DO)
- Financial Crimes Enforcement Network (FinCEN)
- Office of Thrift Supervision (OTS)
- Treasury Inspector General for Tax Administration (TIGTA)

- Additional minor discrepancies were noted in the certification and accreditation documentation at the Bureau of Public Debt (BPD) and the Financial Management Service (FMS). Specifically, missing components required by the National Institute of Standards and Technology components were not included in the documentation.

- Treasury should continue to enforce annual security awareness efforts, specialized security training, and peer-to-peer security training requirements to ensure that all employees, contractors and personnel with significant security responsibilities receive sufficient training. Training improvements are needed for the following bureaus:

  - DO
  - FinCEN
  - Mint

- Treasury should continue to track IT security weaknesses in the plan of action and milestones (POA&M) documents submitted to OMB. Additional improvements with the POA&M process are needed to consistently identify weaknesses from Treasury and OIG reports in the POA&Ms. Additionally, Treasury should ensure that weaknesses identified in the POA&Ms are prioritized to allow appropriate delegation of resources as required by FISMA. Enhancements are needed in the POA&M process at the following bureaus:

  - TTB
  - BEP
  - CDFI

[2] Not all issues were noted at each bureau. Additionally, a full review of the certification and accreditation package information was only performed at BEP, BPD, DO, FMS, OCC, MINT and TTB. For the remaining bureaus, the only procedures performed were follow up activities related to prior year findings.

- DO
- FinCEN
- OCC
- Mint
- TIGTA

- Improvements are needed to ensure that the DO and OCC are adequately identifying system interfaces and documenting supporting connection agreements. Additionally, FMS should ensure that TOP system interfaces are accurately documented in and reconcile between the security plan and the system inventory.

- Treasury should continue to perform security self assessments in accordance with NIST Special Publication 800-26 and NIST Special Publication 800-53. However, specific improvements are needed, as several bureaus did not complete security self assessments during FY 2006. Additionally, several bureaus did not sufficiently address all of the critical elements prescribed by NIST. Improvements are needed at OTS to enhance the security self assessment process.

- Improvements are needed to enhance Treasury's methodologies for categorizing systems in accordance with FIPS 199. We found that Treasury was not fully in compliance with OMB's current requirement to include all systems in the FISMA report and to categorize these systems by FIPS 199 impact risk impact levels. We noted that the bureaus had inconsistent treatments for minor applications. Specifically, BEP and OCC did not identify minor systems in the security plans of their respective parent systems, thus the evaluation team was unable to verify their FIPS 199 categorization. Additionally, Mint and TTB did not identify the ratings assigned to confidentiality, integrity, availability, and overall security, thus the FIPS 199 categorization could not be verified by the evaluation team.

- Improvements are needed to enhance the configuration management process. Specifically, BPD, FinCEN, and OCC have not developed overall configuration policies. For those bureaus that have created overall configuration policies, the specific platforms in use have not been identified. In addition, BEP, DO, FinCEN, Mint, OCC, and OTS have not developed configuration guidelines for each individual operating system and/or platforms used by the agency. Lastly, several bureaus have not developed procedures for determining the implementation percentages of configuration guides.

- Improvements are needed to enhance the incident response process. Specially, several bureaus have not documented their bureau level Computer Security Incident Response Capability (CSIRC) procedures in accordance with guidance outlined in NIST Special Publication 800-61. Specifically, for the following bureaus:

  - TTB
  - DO
  - Mint
  - FinCEN
  - OTS

- TIGTA

Despite these above identified needs for improvement, our FISMA evaluation also showed that Treasury made improvements with its information security program during FY 2006. The following summarizes these improvements:

- Significant improvements have been made in the area of security awareness training and specialized IT training. Specially, the number of individuals who have not attended IT security awareness training has significantly decreased. Additionally, the number of individuals with significant security responsibilities who have attended specialized IT training has increased to near complete compliance during FY 2006.

- All bureaus have addressed peer-to-peer file sharing in their IT security awareness training programs.

- The OCIO has taken steps to ensure a consistent systems inventory is maintained by all bureaus. For example, the OCIO issued several memos to bureau CIOs containing guidance on developing a systems inventory for FISMA reporting purposes. Based on this guidance, the evaluation team identified a more consistent systems inventory then in previous years.

Conclusion

Based on the results of our testing, we believe that, despite several improvements, non-IRS Treasury remains in substantial non-compliance with FISMA. The detailed results for the IRS are contained in the TIGTA's FISMA report.

Overview of TIGTA Evaluation

The TIGTA report provides an independent evaluation of the status of IT security at IRS. The report notes that FY 2006 FISMA results and the results of audits indicate that additional improvements are needed for the IRS to adequately protect the information and systems that support its operations.

The TIGTA noted that during FY 2006 IRS made strides towards improving security; for example:

- IRS re-assessed the security risks of each of its systems;
- The IRS Security Program Management Office Council, with participation from all IRS business units, continued their weekly meetings to plan and refine processes for FISMA compliance;
- The IRS made significant improvements in the security certification and accreditation process; and
- The IRS continued to work closely in seeking guidance and concurrence on FISMA issues with TIGTA and the OCIO to improve compliance with the National Institute of Standards and Technology (NIST) and FISMA Requirements.

Seven areas of concern were highlighted:

- Systems inventory

The IRS reported on its total inventory of 264 systems. In addition, during the 2006 review period, the Office of Mission Assurance and Security Services, in coordination with each of the business units, re-evaluated the risk of all 264 systems. The risk categorization forms the basis for selecting an appropriate set of security controls to protect the confidentiality, integrity and availability of systems and data. TIGTA is confident that the systems inventory is substantially complete and the risk categorizations for IRS systems are accurate.

- Certification and accreditation

The IRS reported having the majority of their systems certified and accredited. The IRS has developed a NIST-compliant process to ensure a thorough assessment of system risk and security for determining whether to accredit a system. However, TIGTA noted problems with the execution of this process. Specifically, application controls were occasionally described as common controls and not tested. Additionally, TIGTA identified examples of controls that were accepted without adequate testing. Lastly, IRS business units did not always track weaknesses identified during the certification process for remediation.

- Continuous monitoring

The IRS has not made progress in implementing annual testing requirements. Self-assessments were conduced on systems not certified during the year; however, the tests were generally conducted on the operating system, and not the application-level controls.

- Tracking corrective actions

TIGTA noted that the IRS process for prioritizing, tracking, and resolving POA&M weaknesses needs significant improvement. Specifically, approximately 75% of both recommendations and proposed corrective actions could not be located by TIGTA in the IRS POA&M. Additionally, the results of a TIGTA issued report were not provide to the IRS business units and not incorporated within the IRS POA&M.

- Security Configuration Policies

The IRS provided configuration guides for all types of operating systems and platforms in operation. However, based on documentation received by TIGTA, the IRS does not appear to have fully implemented the configuration policies for each operating system and platform.

- Incident Reporting Procedures

The IRS is not in compliance with incident reporting policies and procedures. Specifically, the loss or theft of laptops and other portable devices is not being reported to the IRS Computer Incident Response Center (CSIRC) and TIGTA.

- Awareness Training

The IRS is not ensuring that all contractors receive security awareness training.

- Training employees with key security responsibilities

The IRS has improved in ensuring that all individuals with significant security responsibilities receive security-related training. The IRS has also implemented a centralized security training tracking solution. However, further improvements are needed to ensure that employee with significant security responsibilities receive sufficient security training.

- Privacy Requirements

TIGTA determined that the IRS did not comply with section 208 of the E-Government Act [3]on privacy requirements. Specifically, the IRS needs to take further actions to conduct evaluations for all systems and applications which collect personal information, and to enhance its processes to better monitor compliance with privacy policy and procedures. Since being identified, the IRS has taken corrective actions to remedy this condition.

[3] E-Government Act of 2002, Public Law No. 107-347, Sec 208 (December 17, 2002)

Background

Title III of the E-Government Act of 2002, enacted on December 17, 2002, is referred to as FISMA. FISMA permanently reauthorized the framework set forth in GISRA, including the annual Treasury security review and independent evaluations. In addition, FISMA included new provisions to further strengthen the security of the Federal government's information and information systems. We performed our FY 2006 evaluation pursuant to FISMA.

To assist agencies in implementing the requirements of FISMA, OMB issued Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 17, 2006. OMB M-06-20 replaced OMB M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated June 13, 2005. FISMA, along with supporting OMB guidance, lays out a framework for annual IT security reviews, reporting, and remediation planning.

Responses to OMB Questions

OMB's FISMA reporting guidance includes a number of questions, and has been organized as follows:

- Question 1 – Self-Assessment of Agency Systems
- Question 2 – Compliance with C&A Requirements
- Question 3 – System Inventory and Oversight of Contractor Systems
- Question 4 – OIG Assessment of the POA&M Process
- Question 5 – OIG Assessment of the C&A Process
- Question 6 – Configuration Management
- Question 7 – Incident Detection and Handling Procedures
- Question 8 – Security Training and Awareness
- Question 9 – Peer-to-Peer File Sharing

The responses to OMB's questions are contained in the attached tables.

If you have any questions regarding the report, please call Tony Hubbard at (202) 533-4324.

Very truly yours,

KPMG LLP

Attachment

Section C: Inspector General. Questions 1, 2, 3, 4, and 5. Department of the Treasury: Question 1 and 2
1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).
To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can: 1) Continue to use NIST Special Publication 800-26, or, 2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53
Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.
2. For each part of this question, identify actual performance in FY 06 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
BEP	High	5	1	0	0	5	1	1	100.0%	1	100.0%	1	100.0%
	Moderate	23	2	2	0	25	2	2	100.0%	2	100.0%	1	50.0%
	Low	9	0	0	0	9	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	62	4	0	0	62	4	4	100.0%	4	100.0%	0	0.0%
	Sub-total	99	7	2	0	101	7	7	100.0%	7	100.0%	2	28.6%
BPD	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	15	0	0	0	15	0	0	0.0%	0	0.0%	0	0.0%
	Low	8	1	0	0	8	1	1	100.0%	1	100.0%	1	100.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	23	1	0	0	23	1	1	100.0%	1	100.0%	1	100.0%
CDFI	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	2	0	0	0	2	0	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	2	0	0	0	2	0	0	0.0%	0	0.0%	0	0.0%
DO	High	28	2	0	0	28	2	0	0.0%	2	100.0%	2	100.0%
	Moderate	11	2	0	0	11	2	2	100.0%	2	100.0%	1	50.0%
	Low	57	5	0	0	57	5	5	100.0%	5	100.0%	5	100.0%
	Not Categorized	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	97	9	0	0	97	9	7	77.8%	9	100.0%	8	88.9%

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
FinCEN	**High**	**3**	**0**	**2**	**0**	**5**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Moderate	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Low	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Not Categorized	**2**	**0**	**0**	**0**	**2**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Sub-total	**5**	**0**	**3**	**0**	**8**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
FMS	**High**	**6**	**0**	**2**	**0**	**8**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Moderate	**33**	**3**	**0**	**0**	**33**	**3**	**3**	**100.0%**	**3**	**100.0%**	**3**	**100.0%**
	Low	**11**	**0**	**0**	**0**	**11**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Sub-total	**50**	**3**	**2**	**0**	**52**	**3**	**3**	**100.0%**	**3**	**100.0%**	**3**	**100.0%**
IRS	High	4	2	0	0	4	2	2	100.0%	0	0.0%	0	0.0%
	Moderate	180	9	6	1	186	10	10	100.0%	5	50.0%	3	30.0%
	Low	73	3	1	0	74	3	3	100.0%	2	66.7%	1	33.3%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**257**	**14**	**7**	**1**	**264**	**15**	**15**	**100.0%**	**7**	**46.7%**	**4**	**26.7%**
Mint	**High**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Moderate	**13**	**1**	**1**	**0**	**14**	**1**	**1**	**100.0%**	**1**	**100.0%**	**1**	**100.0%**
	Low	**28**	**1**	**0**	**0**	**28**	**1**	**1**	**100.0%**	**1**	**100.0%**	**1**	**100.0%**
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Sub-total	**41**	**2**	**1**	**0**	**42**	**2**	**2**	**100.0%**	**2**	**100.0%**	**2**	**100.0%**

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
OCC	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	10	0	0	0	10	0	0	0.0%	0	0.0%	0	0.0%
	Low	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	135	7	0	0	135	7	7	100.0%	7	100.0%	0	0.0%
	Sub-total	146	7	0	0	146	7	7	100.0%	7	100.0%	0	0.0%
OIG	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Total	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
OTS	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	16	0	0	0	16	0	0	0.0%	0	0.0%	0	0.0%
	Low	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Total	17	0	0	0	17	0	0	0.0%	0	0.0%	0	0.0%
TIGTA	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	8	0	0	0	8	0	0	0.0%	0	0.0%	0	0.0%
	Low	3	0	0	0	3	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	5	0	0	0	5	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	16	0	0	0	16	0	0	0.0%	0	0.0%	0	0.0%

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
TTB	**High**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Moderate	**17**	**1**	**0**	**0**	**17**	**1**	**1**	**100.0%**	**1**	**100.0%**	**1**	**100.0%**
	Low	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Sub-total	**18**	**1**	**0**	**0**	**18**	**1**	**1**	**100.0%**	**1**	**100.0%**	**1**	**100.0%**
Agency Totals	**High**	46	5	4	0	50	5	3	60.0%	3	60.0%	3	60.0%
	Moderate	329	18	10	1	339	19	19	100.0%	14	73.7%	10	52.6%
	Low	192	10	1	0	193	10	10	100.0%	9	90.0%	8	80.0%
	Not Categorized	205	11	0	0	205	11	11	100.0%	11	100.0%	0	0.0%
	Total	772	44	15	1	787	45	43	95.6%	37	82.2%	21	46.7%

Question 3		
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.		
3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 and/or NIST 800-53 requirements by a contractor or other organization is not sufficient; however, self-reporting by another Federal agency may be sufficient. Response Categories: Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time -	- Frequently, for example, approximately 71-80% of the time
3.b.1.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Response Categories: Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete -	Approximately 51-70% complete -

Question 3	
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.	
If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.	Missing Agency Systems: All agency systems were accounted for on the inventory. However, three bureaus did not did not list all interfaces on their inventory for the systems we selected, including: **FMS** - TOP (Major) **OCC** - Shared National Credit Reporting System (Minor) - 401(k) Enrollment (Minor) - Examiner Library/e-Files (Minor) - Appeals Tracking (Minor) - IT Provider Data Mart (Minor) - Management and Accountability Reporting Tools System (Minor) - Training Administration System (Minor) **DO** - Employee Entry Exit System (EEE) (Major) - Treasury Self Administration System (TSAS) (Major) - OFAC Consolidated Technology System (OCTS) (Major) - Confidential Financial Disclosure (CFDT) – Child of DO LAN (Minor) - Configuration Control Board (CCB) – Child of DO LAN (Minor) - Library Acquisition (eSubscriptions) – Child of DO LAN (Minor) - TECHLIB – Child of DO LAN (Minor) - Tracks FOIA requests and produces reports (FOIA) – Child of DO LAN (Minor) - Joint Audit Management Enterprise System (JAMES) – Child of FARS (Minor)
	Missing Contractor Systems: All contractor systems reconciled between the OCIO and bureaus with one exception: **DO** Digital Telecommunications Services v.2 (DTS2)

Question 3		
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.		
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	No

Question 4		
Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below. For items 4a.-4.f, the response categories are as follows: Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time -		
4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Mostly, for example, approximately 81-95% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	- Sometimes, for example, approximately 51-70% of the time
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% of the time
4.e.	OIG findings are incorporated into the POA&M process.	- Mostly, for example, approximately 81-95% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Almost Always, for example, approximately 96-100% of the time
Comments: **Question 2.b. - The IRS reported 61% of its systems were tested and evaluated in 2006. The IRS considered systems that had been certified and accredited within the reporting period as having been tested and evaluated. Using the same criteria we are reporting that 46.6 % (7 of the 15 systems we reviewed) were tested and evaluated. We attribute the difference to the limited number of systems we reviewed in our sample. We did note that the IRS completed self-assessments during the review period for the remaining 8 systems; however, we are not recognizing self-assessments as a method of testing and evaluation. As we reported for FISMA 2005, self-assessment performance levels for applications are often based on tests of the General Support Systems which are usually conducted by the office of the CIO. We recognize these tests are useful. However, application-specific controls have not yet been selected and tested for each application as part of annual testing requirements, and business units have not been adequately involved in the testing. The IRS expects to have annual testing procedures in place in**		

2007. In our 2005 FISMA assessment, we reported our concern that the IRS and State agencies do not use NIST guidelines to monitor the security of federal tax information provided to the State agencies. We did not follow up on this concern during this 2006 assessment; however, we have an audit planned for FY 2007 to further address this issue. Question 3.a. - In 2006, the IRS certified 4 of 7 (57.14%) of its contractor systems and performed self assessments for the other 3 contractor system. As explained in the comments for Question 2.b. we do not recognize self assessments as meeting the annual testing requirement. Therefore, we replied that the IRS provides oversight and evaluation of its contractor systems only Sometimes (51-70% of the time). Question 4.a.-e. - The IRS has developed, implemented, and is managing an agency-wide POA&M process; however, the process needs improvement to ensure that all weaknesses are tracked in the repository the IRS uses to generate POA&Ms. From 9 TIGTA security reports issued during the 2006 FISMA reporting period, we could locate only 11 of 41 (26.8%) recommendations and 11 of 47 (23.4%) proposed corrective actions in the weakness repository. The repository also contained no weaknesses for 2 applications of a sample of 10 certified and accredited in 2006 even though control weaknesses were identified during the certification. We located a POA&M for one of the two systems, indicating that the POA&M was not generated from the weakness repository contrary to IRS POA&M procedures. In addition, in September 2005, the TIGTA issued audit report 2005-20-143, titled, The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made. We reported that problems identified during vulnerability scans and penetration tests were not formally provided to the business owners, and corrective actions were not documented in POA&Ms. If all weaknesses are not entered into the weakness repository, IRS cannot ensure that POA&Ms are developed and corrective actions are taken to address security weaknesses.

Question 4.e - No OIG Reports were conducted in FY 2006. Therefore, findings were not incorporated into the POA&M process.

Question 5

OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans .

	Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing -	- Poor

Comments: We reviewed a statistical sample of 30 non-IRS treasury major and minor applications, and general support systems, from DO, BEP, BPD, FMS, Mint, OCC, and TTB during FY 2006. During our review, we noted that significant improvements still need to be made to the certification and accreditation processes used by the Department of the Treasury. While a process for the certification and accreditation of major and general support systems that follows the guidance outlined in NIST 800-37does exist at the majority of bureaus evaluated, weaknesses were identified in key documentation supporting the process. Specifically, we identified several missing key components required by NIST SP 800-18, 800-30, and 800-34 for the system security plans, risk assessment, and the contingency plan of each major application or general support system reviewed. Additionally, for any minor systems selected, we noted that the system has not been mentioned in the key certification and accreditation documentation of its parent system.

IRS Comment - We reviewed a sample of 10 applications that were certified and accredited during 2006. The IRS made substantial improvements to the C&A process during the 2006 FISMA reporting period. They have implemented a repeatable, NIST-compliant process designed to ensure a thorough assessment of system risk and security from which the system owner can make an appropriate accreditation decision. While we recognize and commend the IRS on this significant progress, the process needs further improvement to support an assessment level exceeding satisfactory. As we reported in Question 2, the IRS has not implemented procedures to ensure the continuous monitoring of security controls, a key requirement of the C&A process. Such procedures would require system owners to select a subset of controls for each system they own, to be tested in the interim years when a system is not scheduled for certification. The selection of controls is a system owner decision and should consider risk as well as the degree to which a control might degrade between certification cycles. The IRS recognizes the need to improve compliance with Continuous Monitoring requirements and has committed to developing a process and guidelines to better implement this control during 2007. In addition, our review of the System Security Plans (SSP) showed application-specific controls that were sometimes described as common or General Support System controls, resulting in the controls not being tested as part of the certification Security Test and Evaluation (ST&E). We also found application-specific controls not tested in the ST&E without a documented reason, as well as examples of

controls with a rating of "PASS" that was not clearly supported. Controls described in the SSP as Partially in Place or Not in Place were not always tracked as a weakness when a risk-based decision had not been made to waive the required control. As mentioned in our comments for question 4, we found that ST&E findings were not always tracked in the weakness repository.

Section B: Inspector General. Question 6, 7, 8, and 9. Agency Name:		
Question 6		
6.a.	Is there an agency wide security configuration policy? Yes or No.	No
	Comments: The overall agency guidelines described in the TD P 85 requires that each bureau document configuration management plans for Information Technology (IT) systems and networks. We evaluated each bureau configuration management plan/policy to determine if the overall agency has addressed configuration management practices. Based on our review, we determined that 8 out of 11 bureaus had finalized configuration management policies. Therefore, all agencies do not comply with TD P 85. Additionally, TIGTA reported that IRS has established an agency wide security configuration policy.	

Section B: Inspector General. Question 6, 7, 8, and 9. Agency Name:			
Question 6			
6.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.		
Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	No	Yes	- Frequently, or on approximately 71-80% of the systems running this software
Windows NT	No	Yes	- Sometimes, or on approximately 51-70% of the systems running this software
Windows 2000 Professional	No	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows 2000 Server	No	Yes	- Sometimes, or on approximately 51-70% of the systems running this software
Windows 2003 Server	No	Yes	- Frequently, or on approximately 71-80% of the systems running this software

Question 6			
Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Solaris	No	Yes	- Frequently, or on approximately 71-80% of the systems running this software
HP-UX	No	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Linux	No	Yes	- Frequently, or on approximately 71-80% of the systems running this software
Cisco Router IOS	No	Yes	- Frequently, or on approximately 71-80% of the systems running this software
Oracle	No	Yes	- Frequently, or on approximately 71-80% of the systems running this software
Other. Specify: SQL, C/A Top Secret, Firewall, Intrusion Detection System (IDS), Virtual Private Network (VPN), Local Area Network (LAN) switch, VMS O/S, Unix RTR, AIX, IBM Z/OS, SQL Server, Macintosh O/S	No	Yes	- Frequently, or on approximately 71-80% of the systems running this software

Comments: While eight of eleven non-IRS Treasury bureaus have implemented a bureau-wide configuration management policy, there is not 100% compliance. Additionally, these policies do not identify or address the individual platforms or technologies in use by each bureau. It should be noted that individual configuration guides have been developed for most platforms in use, however several bureaus have still not developed configuration guides for various versions of Microsoft Windows, Cisco IOS, and Oracle.

Additionally, the overall conclusion for non-IRS bureaus on the questions of "Is there an agency wide security configuration policy" and "Is [the product] addressed in agency-wide policy" was determined to be "No". However, TIGTA reported an answer of "Yes" for both questions at IRS. Since IRS operates approximately 33% of the agency's system, the answer to both questions over all was concluded to be "No".

IRS Comments: IRS reported that Windows 2000 Professional and HP-UX are not in use.

IRS Comments: Our assessment differs from IRS' assessment for systems running Linux and Oracle software. For each of these, IRS reported an implementation rate of, "Mostly, or on approximately 81-95% of the systems running this software", while we rated the two as, "Rarely, or, on approximately 0-50% of the systems running this software". Our ratings reflect that IRS could not provide documentation of testing done to support the extent to which the security configuration policy has been implemented on the systems running Linux, or Oracle.

Question 7		
Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.		
7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes
IRS Comments: Questions 7.a. & b. - The IRS has not followed policies and procedures for reporting incidents internally or to law enforcement authorities. The IRS responded that they have followed incident reporting policies and procedures. Our response is based on a separate, on-going audit in which we found that incidents involving lost or stolen computer devices (e.g., laptops, blackberries) were not reported to IRS' CSIRC or the TIGTA. However, we noted that the remaining non-IRS Treasury bureaus do follow documented policies and procedures for reporting incidents both internally and to external law enforcement authorities.		

Question 8		
8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training
Comments: While TIGTA reported an overall rating of "Sometimes, or approximately 51-70% of employees have sufficient training" for IRS, the non-IRS Treasury bureaus were determined to be between 80% to 99% compliance with security awareness training and awareness, as well as specialized training for employees with significant IT security responsibilities. **IRS Comments: We are supplementing this response with comments because a single response choice cannot be applied to the two separate performance measures addressed in Question 8; namely, awareness training for all employees (including contractors) as well as specialized security training for employees with significant security responsibilities. Awareness training - IRS provided security awareness training to all employees and contractors during the 2006 reporting period. Specialized security training - We are reporting that 69% (1,711 of 2,476) of employees with significant security responsibilities received specialized security training during the evaluation period. We disagree with the IRS' response that 99% (2,447 of 2,476) of these employees received specialized security training. We determined that 29% (719 of the 2,476) of the employees trained received less than 8 hours of specialized training. We do not agree that training of less than 8 hours meets this security requirement.**		

Question 9		
9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

Appendix A Treasury Bureaus

Treasury is comprised of the following 13 bureaus and offices for FISMA reporting purposes:

- Alcohol and Tobacco Tax and Trade Bureau (TTB);
- Bureau of Engraving and Printing (BEP);
- Bureau of Public Debt (BPD);
- Community Development Financial Institutions Fund (CDFI);
- Departmental Offices (DO);
- Financial Crimes Enforcement Network (FinCEN);
- Financial Management Service (FMS);
- Internal Revenue Service[4] (IRS);
- Office of the Comptroller of the Currency (OCC);
- Office of Inspector General (OIG);
- Office of Thrift Supervision (OTS);
- United States Mint (Mint); and,
- Treasury Inspector General for Tax Administration (TIGTA).

[4] The IRS FISMA evaluation is performed by TIGTA.

Appendix B Abbreviations

ASAP	Automated Standard Application for Payments – *FMS System*
BCP	Business Continuity Plan
BATS	Bureau Automated Tracking System – *FMS System*
BEP	Bureau of Engraving and Printing
BEPMIS	BEP Management Information System – *BEP System*
BPD	Bureau of Public Debt
C&A	Certification & Accreditation
CDFI	Community Development Financial Institutions Fund
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations Plan
COTR	Contracting Officer Technical Representative
CSIRC	Computer Security Incident Response Center
DAA	Designated Approving Authority
DATS	Deficiency Abatement Tracking Systems – *BEP System*
DCI	Digital Check Imaging – *FMS System*
DO	Departmental Organization
DRP	Disaster Recovery Plan
EEE	Employee Entry Exit System – *DO System*
ECP	Electronic Check Processing – *FMS Systems*
EFTPS	Electronic Federal Tax Payment System – *FMS System*
ESS	Engraving Support System – *BEP System*
FARS	Financial Analysis Reporting System – *DO System*
FCAS	Foreign Currency Accounting System – *FMS System*
FinCEN	Federal Crimes Enforcement Network
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMS	Financial Management Service
FY	FISMA Year
GISRA	Government Information Security Reform Act
GSS	General Support System
IRIS	Integrated Revenue Information Systems – *TTB system*
IRS	Internal Revenue Service
ISA	Interconnection Security Agreements
IT	Information Technology
JAMES	Joint Audit Management Enterprise System – *DO System*
LAN	Local Area Network
LMS	Learning Management System – FMS System
MFDT	MoneyFactory DataTools Web Infrastructure – *BEP System*
Mint	United States Mint
MOU	Memorandum of Understanding
MUTS	Mutilated Currency Tracking System – *BEP System*
TMWI	TIGTA Microsoft Window's Infrastructure – *TIGTA System*
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OCIO	Office of the Chief Information Officer

OFF	Oracle Federal Financials
OIG	Office of Inspector General
OMB	Office of Management and Budget
OST	Office of Security Training Management System – *BEP System*
OTS	Office of Thrift Supervision
PACS	Patriot Act Communication System – *FinCEN System*
POA&M	Plan of Action & Milestones
PSMS	Police Supply Management System
RS2	Retail Sales System – *Mint System*
SIA	System Interface Agreement
ST&E	Security Test & Evaluation
STS	Schedule Transfer Service – *BEP System*
TACT	Treasury Assignment and Correspondence Tracking - *DO System*
TCS	Treasury Communications System
TCSIRC	Treasury Computer Security Incident Response Center
TECS	Treasury Enforcement Computer System
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
TSAS	Treasury Self Administration System
TSDS	Technical Security Division Systems – *BEP System*
TOP	Treasury Offset Program – *FMS System*
TTB	Alcohol and Tobacco Tax and Trade Bureau
US-CERT	United States Computer Emergency Readiness Team
WCF	Western Currency Facility

Appendix C Objective, Scope, and Methodology

The objective of our evaluation was to determine the effectiveness of Treasury's information security program and practices, as it relates to non-national security systems for the following 12 bureaus and offices: BEP, BPD, CDFI, DO, FinCEN, FMS, OCC, OIG, OTS, Mint, TIGTA, and TTB. Note that TIGTA conducts a separate FISMA evaluation for the IRS, as FISMA mandates an evaluation by both the Treasury OIG and TIGTA.

On July 17, 2006, OMB issued Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act*. Section A of M-06-20, *Instructions for Completing the Annual FISMA Report and Privacy Management Report*, contains instructions and frequently asked questions to aid Federal CIOs, OIGs, and Senior Agency Officials for Privacy, in preparing and submitting the FY 2006 FISMA Report and the Privacy Management Report. Section C of M-06-20, *Reporting Template for Agency IGs*, contains specific instructions for IGs to complete the FY 2006 FISMA template.

In addition, OMB's FISMA guidance states that "IGs or their designee, perform an annual independent evaluation of the information security program and practices of the agency to determine the effectiveness of such program and practices." Further, it states "the evaluation shall include testing of the effectiveness of information security policies, procedures and practices, to make an assessment of the compliance with information technology security policies, procedures, standards and guidelines. The testing should include an appropriate subset of agency systems. In this regard, FISMA does not limit the subset to financial systems."

To meet the requirements of FISMA, and to conform with OMB's guidance, we performed the following evaluation procedures:

- Followed up on issues identified during the FY 2005 FISMA evaluation.
- Submitted information requests to the CIO and/or Treasury components.
- Reviewed Treasury's FY 2006 FISMA submission.
- Reviewed data and documentation provided to us by Treasury, including documentation for the following subset of systems.
  - BEP IBM 2066 Mod A01 z800 eServer
  - BEP 103103-MFDT
  - BEP 260010-MUTS
  - BEP 107106-DATS
  - BEP 700511-STS
  - BEP 520112-OST
  - BEP 520114-PSMS
  - BPD Bureau Automated Tracking System (BATS)
  - DO Tracks FOIA request and produces reports
  - DO Confidentiality Financial Disclosure system
  - DO Configuration Control Board system
  - DO Library Acquisition (eSubscriptions)
  - DO Employee Entry Exit System (EEE)

- DO TECHLIB
- DO Joint Audit Management Enterprise System (JAMES)
- DO OFAC Consolidated Technology System (OCTS)
- DO Treasury Self Administration System (TSAS)
- FMS Automated Standard Application for Payments (ASAP)
- FMS Electronic Check Processing (ECP)
- FMS Treasury Offset Program (TOP)
- Mint General Support System (GSS)-Local Area Network (LAN-Philadelphia)
- Mint Service Software – oid32031 – Blackberry Enterprise Server
- OCC Shared National Credit Reporting System
- OCC 401(k) Enrollment
- OCC Examiner Library/e-Files
- OCC Appeals Tracking
- OCC IT Provider Data Mart
- OCC Management and Accountability Reporting Tools System
- OCC Training Administration System
- TTB Integrated Revenue Information System (IRIS)

- Incorporated the IRS FISMA evaluation information provided by TIGTA.
- Reviewed other relevant material (e.g. NIST guidance and Treasury OIG reports).
- Interviewed key Treasury officials.

The evaluation was conducted in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*, issued January 2005, and subsequent revisions.

Appendix D Comments on Questionnaire Numbers

Question 1 – Self-Assessment of Agency Systems

CIO: The CIO's office maintains an inventory of each bureau's major applications and general support systems that have been certified and accredited. No exception noted.

The evaluation team inspected bureau self-assessments and the methodologies used to conduct self-assessments. The evaluation team also met with each of the 11 non-IRS bureaus to gain an understanding of the methodologies used to create their system inventories. Lastly, the evaluation team verified the bureaus' FIPS 199 systems categorization efforts. The results have been included below:

- BEP – The evaluation team inspected the system security plans for the IBM 2066 Mod A01 z800 eServer and the BEP Local Area Network (of which 260010-MUTS, 103103-MFDT, 107106-DATS, 520114-PSMS, 700511-STS, and 520112-OST are child systems). The FIPS 199 categorization applied to the IBM 2066 Mod A01 z800 eServer appears to be appropriate based on the confidentiality, integrity, availability, and overall security ratings assigned to the system. However, the evaluation team was unable to identify any reference to MUTS, MFDT, DATS, PSMS, STS, and OST, and thus was unable to verify the appropriateness of the FIPS 199 categorization for each child system. The evaluation team also noted that a self-assessment or form or security control testing was performed over the IBM eServer, MUTS, DATS, PSMS, STS, OST and TSD in accordance with the guidance outlined in NIST Special Publication 800-26 in FY 2006. The evaluation team also noted that MUTS has been reported on the bureau's inventory, however the system is currently in development. Lastly, we noted that sixty-two BEP systems have yet to receive a FIPS 199 categorization. **Exceptions Noted.**

- BPD – The evaluation team inspected the self-assessment documentation for the BATS system and determined that a self-assessment was performed in accordance with the guidance outlined in NIST Special Publication 800-53A. The evaluation team also inspected the BATS system security plan and determined that it has been appropriately granted a FIPS 199 categorization of low. No exceptions noted.

- CDFI – The evaluation team did not identify any discrepancies or issues with the bureaus' system inventory or assessment of security controls. No exceptions noted.

- DO – The evaluation team noted that DO has categorized five minor child systems on their inventory as high according to FIPS 199. Guidance established by the OCIO in the FISMA Systems Inventory and Classified Systems Data Call Memo requires that all systems with a FIPS 199 categorization of high be classified as a major application. DO has also included the OFAC Consolidated Technology System (OCTS) on their inventory, however this system was in the development stage at the time of fieldwork. Additionally, the evaluation team determined that the systems JAMES and EEE have not received an appropriate FIPS 199 categorization. NIST Special Publication 800-37 requires that systems be given an overall security rating equivalent to the highest rating for the system's confidentiality, integrity, and availability, which is high for both of these systems. In addition, TSAS has been assigned a FIPS 199 categorization without the performance of a certification and accreditation. **Exception Noted.**

- FinCEN – The evaluation team noted that the FinCEN Database and Case Management systems have not been assigned a FIPS 199 categorization. FIPS 199 requires that all systems be categorized with a high, medium or low rating. **Exceptions Noted.**

- FMS – The evaluation team inspected the system security plans for the ASAP, ECP, and TOP systems and noted that the FIPS 199 categorizations of each system appear to be appropriate based on the confidentiality, integrity, availability, and overall security rating assigned to each system. The evaluation team determined that a self-assessment was performed on the ECP system in accordance with the guidance outlined in NIST Special Publication 800-53, however a self-assessment was not performed on the Automated Standard Application System (ASAP) and the Treasury Offset Program (TOP) system. Instead, a security assessment of these two systems was performed in FY 2006. The evaluation team was informed by FMS that a self-assessment is not performed on a system in a year that a security assessment is performed. No exceptions noted.

- Mint – The evaluation team inspected the system security plans for the General Support System (GSS) – Local Area Network (LAN- Philadelphia) and Blackberry Enterprise Server and noted that the FIPS 199 categorization for the GSS – LAN Philadelphia appears appropriate based on the confidentiality, integrity, and availability rating assigned. However, the evaluation team was unable to determine the confidentiality, integrity, availability, and overall security rating assigned to the Blackberry Enterprise Server from the system security plan of the parent system, the Mint LAN GSS. The evaluation team inspected the self-assessments for the GSS-LAN Philadelphia and the Mint LAN GSS and noted that a self-assessment has been performed on the Mint LAN GSS, and GSS-LAN Philadelphia using the guidance outlined in NIST Special Publication 800-26. **Exception Noted.**

- OTS – While no systems were selected at OTS as part of the FY 2006 FISMA assessment, the evaluation team followed up on a prior year finding and identified that the bureau did not perform a self-assessment for the ADM200 Personnel/Payroll system during the FISMA year. **Exception Noted.**

- OCC – The evaluation team reviewed the system security plans for the Examinations system (selected child systems: Shared National Credit Reporting system, Examiner/e-Files system, and the IT Provider Data Mart), the Fiscal Management system (selected child systems: Management and Accountability Reporting Tools system and Training Administration system), the Workforce Operations system (selected child system: 401(k) Enrollment system), and the Ombudsman system (selected child system: Appeals Tracking system) and noted that no child systems have been identified in the security plans of their respective parent systems. In addition, the evaluation team followed up on a prior year finding to determine if the Risk Analysis system has been categorized with a FIPS 199 rating. The Risk Analysis system has been assigned a categorization of Low; however, this rating has not been reflected in the system's security plan. As a result, the FIPS 199 categorizations of each selected system could not be verified. In addition, none of the minor child systems within the OCC's inventory are categorized according to FIPS 199. The evaluation team was informed that OCC has a self-assessment methodology that follows the guidance outlined in NIST Special Publication 800-26; however, self-assessments are not required for minor systems. Only minor systems were selected as part of our subset of systems at OCC. **Exception Noted.**

- TIGTA – The evaluation team identified three (3) discrepancies in the system inventory reported by TIGTA. First, the MOM minor child system has been reported on the bureau's inventory; however, this system is currently in development. Second, the SNA[5] system has been reported on the bureau's inventory; however, this system is owned and operated by the United States Department of Homeland Security Customs and Border Protection (CBP). Third, five (5) systems have not received a FIPS 199 categorization. Lastly, the evaluation team also noted that TIGTA is using the guidance outlined in NIST Special Publication 800-26 for conducting self-assessments of all applicable systems. **Exception Noted.**

- TTB – The evaluation team inspected the system security plan for the Integrated Revenue Information System (IRIS) and noted that the confidentiality, integrity, availability, and overall security rating have not been included in the plan. As a result, the evaluation team was unable to verify the FIPS 199 categorization of the system. The evaluation team then inspected the self-assessment methodology developed by TTB and concluded that the IRIS system was assessed in FY 2006 using the guidance outlined in NIST Special Publication 800-26. **Exception Noted.**

Summary: Based on the scope of this review, Treasury should ensure that self assessments are be performed annually. In addition, improvements should be made to ensure that Treasury is consistently assigning FIPS 199 ratings that correspond to the system's confidentiality, integrity, availability, and overall security ratings as documented in the systems' security plans and other certification and accreditation documentation.

Question 2 – Compliance with C&A Requirements

- The evaluation team reviewed certification and accreditation data provided for the subset of agency systems selected as part of this year's assessment. The data provided included the numbers of systems with certifications and accreditations, the number of systems for which controls had been tested and evaluated within the last year, and the number of systems that had tested contingency plans. The evaluation team also inspected documentation to determine if the systems' contingency plans had been tested during the FISMA year. Additionally, the evaluation team inspected the bureau certification and accreditation schedules to determine if the authorities to operate were current and had been revised as required. The results have been included below:

  - BEP – The evaluation team reviewed the BEP Certification and Accreditation Schedule and noted that all systems we selected had been a certified to operate. The evaluation team also reviewed the System Inventory Database and noted that the contingency plans for the MUTS, PSMS, DATS, STS, and OST have not been tested in the past year. The evaluation team also reviewed the System Inventory Database and noted that the security controls for the MUTS, PSMS, DATS, STS, and OST have been tested in the past year. Each of these systems are children of the BEP LAN. Based on follow up activities related to a prior year finding, the evaluation team also noted that the TSD Continuity of Operations (COOP) had not been finalized. **Exception Noted.**

[5] SNA was listed on the TIGTA systems inventory as a system. However, this item is only the interface to another system called the Treasury Enforcement Computer System (TECS). TECS should have been listed on the TIGTA system inventory.

- BPD – The evaluation team reviewed the BPD Systems Inventory and noted that the contingency plans for all systems selected had been tested in the past year. In addition, the evaluation team reviewed the BPD Certification and Accreditation Schedule and noted that all systems have either been certified or accredited, or have a certification and accreditation in process. No exceptions noted.

- CDFI – The evaluation team inspected the Systems Inventory and Certification and Accreditation Schedules for CDFI and noted no exceptions.

- DO – The evaluation team reviewed the DO Systems Inventory and noted that eight systems of the nine systems selected for review have had their contingency plan tested in the current year. The evaluation team also noted that the contingency plan of the JAMES system, a child of the FARS system, had not been tested in the current year. The evaluation team followed up on a prior year finding related to the testing of the contingency plan for the DO TACT system and noted that the plan had not been testing in FY 2006. The evaluation team reviewed the certification and accreditation schedule and compared to the inventory. **Exceptions Noted.**

- FinCEN – The evaluation team inspected the Systems Inventory and Certification and Accreditation Schedules for FinCEN and noted no exceptions. However, the evaluation team followed up on a prior year finding related to the testing of the contingency plan for the FinCEN ITI and noted that the plan had not been tested in FY 2006. **Exception Noted.**

- FMS – The evaluation team inspected the FMS Systems Inventory to gain an understanding of the number of systems that been certified and accredited, have had security controls tested within the past year, and have had the system's contingency plan tested. The evaluation team determined that of the three systems selected as part of our subset of systems (ASAP, ECP, and TOP); all have had their security controls; complete certification and accreditations, as well as, contingency plans tested within the past year. No exceptions noted.

- Mint – The evaluation team inspected the U.S. Mint System Inventory to gain an understanding of the number of systems that have been certified and accredited, have had security controls tested within the past year, and have had the system's contingency plan tested. The two U.S. Mint systems selected as part of our subset of bureau systems were the GSS-LAN Philadelphia and the Blackberry Enterprise Server. The evaluation team determined that both have been certified and accredited and have had the system contingency plan tested within the past year. In addition, the evaluation team identified that security controls for the Blackberry Enterprise Server and GSS-LAN Philadelphia have been tested within the past year. Additionally, the evaluation team reviewed the Certification and Accreditation Schedule and noted that all other U.S. Mint systems have been certified and accredited. No exception noted.

- OCC – The evaluation team inspected the OCC system inventory to gain an understanding of the number of systems that have been certified and accredited, have had security controls tested within the past year, and have had the system's contingency plan tested. For the seven OCC systems selected, the Shared National Credit Reporting system, IT Provider Data Mart system, the Examiner Library/e-File system (child systems of the Examiner system), the Management and Accountability Reporting Tools system and Training Administration system (child systems of the Fiscal Management system), the 401(k) Enrollment system (child system of the Workforce Operations system, and the Appeals Tracking system (child system of the Ombudsman system),

the evaluation team noted that each has been certified and accredited and had their security controls evaluated in the past year. However, of the seven systems selected, none have had their or their parent system contingency plans tested within the past year. The evaluation team also reviewed the OCC Certification and Accreditation Schedule and noted that all systems, including the seven systems selected as part of our subset, have been certified and accredited. **Exception Noted.**

- OTS – The evaluation team inspected the systems inventory and certification and accreditation schedules for OTS and noted no exceptions

- TIGTA – The evaluation team inspected the systems inventory and certification and accreditation schedules for TIGTA and noted no exceptions.

- TTB – The evaluation team reviewed the TTB Systems Inventory and noted that the Integrated Revenue Information System (IRIS) has been certified and accredited, has had its security controls tested within the past year, and has had its contingency plan tested within the past year. The evaluation team also reviewed the TTB Certification and Accreditation Schedule and noted that all selected systems are currently certified and accredited. No exceptions noted.

Summary: Based on the scope of the review, we concluded that Treasury should continue to test capabilities to restore operations following a disaster, and continue to make sure there is adequate supporting documentation for such efforts. Additionally, Treasury should ensure that Certification and Accreditation Schedules are documented to ensure that the system certification and accreditations are current and have been updated as required. Lastly, Treasury should ensure that each system's security controls are tested on an annual basis.

Question 3 – System Inventory and Oversight of Contractor Systems

- CIO – The evaluation team performed a comparison of the bureau system inventories to the Office of the Chief Information Officer (OCIO) consolidated system inventory. Several minor discrepancies in the inventory reported by the bureaus versus the consolidated inventory maintained by the OCIO were identified. In one instance, two (2) FINCEN systems and five (5) DO systems were categorized with a FIPS 199 rating of high. In another instance, a child system of TIGTA was not accounted for in the OCIO's consolidated inventory. In another instance, the OCIO included two systems that were not identified or accounted for by DO. The last instance dealt with a difference in categorization of systems between the OCIO and FMS. **Exception Noted.**

- The evaluation team also inspected bureau FISMA submissions to determine which Treasury bureaus reported having contractor systems. Based on this review, the evaluation team noted that BEP and Mint reported one contractor system each. Additionally, FinCEN and FMS each reported three contractor systems. No other bureaus reported contractor systems. Thus, the evaluation team inspected the contracts for BEP, FinCEN, FMS and Mint, and performed inquiry and document inspection to determine whether contractor oversight was adequately performed. The results for testing at BEP, FinCEN, FMS, and Mint have been included below:

  - BEP –Upon a reconciliation of the BEP systems inventory to the consolidated inventory reported by the OCIO, the evaluation team identified a minor discrepancy. BEP has reported twenty-two moderate and sixty-two non-categorized systems, however the OCIO consolidated inventory

displays twenty-three moderate systems and sixty-one non-categorized systems. The evaluation team also noted that BEP reported one contractor system. Grey Hawk Systems, Inc. provides web hosting and maintenance services. **Exception Noted.**

- FinCEN – Upon a reconciliation of the bureau's inventory to the consolidated inventory reported by the OCIO, the evaluation team identified a minor discrepancy. FinCEN has reported two non-categorized minor child systems, however the OCIO consolidated inventory is reporting two high minor child systems. The evaluation team noted that FinCEN reported three contractor systems: the 314(a) system, the Patriot Act Communication System (PACS), and the FinCEN Home Website. Service for each of these systems is provided via the Treasury Communications System (TCS). A Memorandum of Understanding for all three systems has been signed by the TCS Designated Approving Authority (DAA) and the FinCEN DAA. The evaluation team also determined that FinCEN performs oversight and conducts evaluations of these three systems in accordance with federally mandated guidelines, including NIST Special Publication 800-26. **Exception Noted.**

- FMS – Upon a reconciliation of the bureau's inventory to the consolidated inventory reported by the OCIO, the evaluation team identified a minor discrepancy. FMS has reported twelve moderate minor systems and six low minor systems, however the OCIO is reporting thirteen moderate minor and five low minor systems. Regarding contractor systems, the evaluation team noted that FMS reported three contractor systems, the Electronic Federal Tax Payment System (EFTPS), CASH-LINKII, and the Learning Management System (LMS). For each contractor system, the evaluation team reviewed Memorandums of Understanding or equivalent documentation and noted that a signed agreement is in place for all contractor systems. The evaluation team also determined that FMS performs oversight of each contractor systems and conducts evaluations in accordance with federally mandated guidelines. No exceptions noted.

- Mint – The evaluation team noted that the U.S. Mint has one contractor system, the Retail Sales System (RS2). The evaluation team identified that a signed Memorandum of Understanding and Interconnection Security Agreement (ISA) exists. No exceptions noted.

- The evaluation team reviewed all systems identified based on the system selection methodology for interface testing. Based on our system selection methodology, systems were selected from only 7 bureaus: BEP, BPD, DO, FMS, Mint, OCC and TTB. We inspected system security plans to determine whether a system interface had been documented for each system. For any interfaces documented in the system security plans, the evaluation team requested the supporting interface connection agreements. The evaluation team also inspected the bureaus' quarterly FY 2006 system inventory submissions to the OCIO, and noted that the system inventories were adequately maintained and updated. Additionally, the evaluation team inspected e-authentication risk assessments as required. The specific results of the test work for the seven bureaus with systems selected are identified below:

  - BEP – Upon inspecting the security plans for the BEP IBM 2066 Model z800 eServer, BEP LAN/WAN, and PSS, the evaluation team noted that each of these systems interface with the FMS LAN/WAM through the Treasury Communication System (TCS), and subsequently the FMS ICCC and Western Currency Facility (WCF). The evaluation team then inspected the BEP Memorandum of Understanding (MOU) and System Interface Agreement (SIA) with FMS and

noted that this document had been signed by both designated approving authorities. No exceptions noted.

- BPD – Upon inspecting the BPD BATS system security plan, the evaluation team noted that system is a stand-alone system that did not connect to any outside networks of the Internet. The evaluation team concluded that the BATS system does not have any interfaces. No exception noted.

- DO –The evaluation team noted that DO has not properly identified system interfaces within their system security plan and system inventory. Specifically, no indication of whether or not an interface exists for a child system exists was presented in the documentation. Additionally, the evaluation team noted that DO was unable to provide any verification of an e-authentication risk assessment for the JAMES system. **Exception Noted.**

- FMS – The evaluation team inspected the system security plan and the interface document for the Automated Standard Application for Payments (ASAP) system and noted that the system's interfaces with the Voice Response System, Cash Track System, TWAI UPS, Certificate Authority, and LDAP systems were included in the ASAP system security plan, but not in the system interfaces document. The evaluation team noted that the TOP security plan did not include external interfaces. Specifically, the evaluation team noted that TOP currently has 20 external interfaces, all with Memorandums of Understanding (MOU). However, each of the 20 external interfaces identified with an MOU have not been identified in the TOP security plan. **Exception Noted.**

- Mint – The evaluation team did not identify any weaknesses in the system interfaces documented from the subset of U.S. Mint systems selected. No exceptions noted.

- OCC – Upon inspecting the security plans for the Examinations system, the Workforce Operations system, and the Fiscal Management system, the evaluation team noted that the Shared National Credit system's interfaces with the KMV Credit Monitoring system and Zeta Subscription Report service. However, these interfaces have not been identified in the bureau's system inventory. The evaluation team also noted that the Examiner Security Plan does do not document any internal or external connections for the Examiner Library/e-Files, IT Provider Data Mart, and Management and Accountability Reporting Tools systems that are documented within the systems inventory listing. Additionally, the evaluation team noted that OCC does not maintain system interconnection agreements for minor systems. **Exceptions Noted.**

- TTB – The evaluation did not identify any weaknesses in the system interfaces documented from the subset of TTB systems selected. No exceptions noted.

Summary: Based on the scope of this review, the evaluation team noted that improvement is needed in regards to documenting connection agreements between all bureaus and agencies. In addition, Treasury should continue to perform contractor oversight to ensure contractors fulfill agreement terms. Finally, Treasury should continue to ensure that each bureau updates and maintains system inventories on a quarterly basis.

Question 4 – OIG Assessment of the POA&M Process

- CIO: The evaluation team was informed that the OCIO is responsible for centrally tracking, maintaining, and reviewing bureau POA&M activities on a quarterly basis. However, the evaluation team noted nine out of eleven bureaus did not document weaknesses identified in the security program weakness identified by the Office of the Chief Information Officer - Office of Cyber Security Oversight and Compliance in the bureau Plan of Actions and Milestones (POA&M) in 2004. **Exception Noted.**

- The evaluation team performed a review of bureau POA&Ms. The evaluation team inspected the POA&Ms to determine if known IT security weaknesses had been incorporated and prioritized. Additionally, the evaluation team inspected security program review and assistance reports and OIG reports to determine if the weaknesses identified in the reports were documented in the POA&Ms. Results of this review have been included below:

  - BEP, CDFI, FinCEN, TIGTA – The evaluation team reviewed IT security weaknesses in the POA&Ms for each of the aforementioned bureaus and noted that the scheduled completion dates for weaknesses were past due. In addition, no change to the milestone date was listed for weaknesses in each bureau's POA&M. **Exception Noted.**

  - BEP – The evaluation team noted that point of contact information for each weakness has not been identified in the bureau's POA&Ms in the third quarter of FY 2006. In addition, unique project identifiers were not included for each weakness listed in the POA&M for the third quarter of FY 2006. **Exception Noted.**

  - BPD – The evaluation team noted that weaknesses had been incorporated and prioritized. In addition, weaknesses identified in the security program review and assistance reports were documented in the POA&Ms. No Exception noted.

  - CDFI – The evaluation team noted that the POA&Ms were not prioritized per guidance outlined by the OCIO. **Exception Noted.**

  - DO – The evaluation team was unable to obtain a POA&M submission for the second quarter of FY 2006. The evaluation team also noted that the scheduled completion date was missing for various weaknesses in the first and third quarters. **Exception Noted.**

  - FinCEN – The evaluation team noted that POA&Ms are not being prioritized. Additionally, the evaluation team also noted that unique project identifiers were not included for each weakness listed in the POA&M. **Exception Noted.**

  - FMS –The evaluation team followed up on a prior year finding regarding the inclusion of OIG report findings into the POA&M. Findings from OIG report OIG-05-041 have been included. The evaluation team noted that all weaknesses have been incorporated and prioritized. No exception noted.

  - Mint – The evaluation team noted that weaknesses listed in the POA&Ms did not include a weakness description for the first and second quarter. In addition, a unique project identifier was

not listed in the POA&M for all three quarters. The evaluation team also followed up on a prior year finding regarding the inclusion of OIG reports into the Mint POA&M and noted that all findings from OIG report OIG-05-040 have still not been included. **Exception Noted.**

- OCC – The evaluation team noted that the scheduled completion dates for weaknesses in the POA&M were altered instead of documenting a milestone change. Additionally, Point of Contact (POC) information for each weakness has not been identified in the bureau's POA&Ms. **Exception Noted.**

- OTS - The evaluation team noted that all weaknesses have been incorporated and prioritized. In addition, weaknesses identified in the security program review and assistance reports were documented in the POA&Ms. No Exception noted.

- TIGTA – The evaluation team noted that scheduled completion dates were missing for various weaknesses. Additionally, Point of Contact information for each weakness has not been identified in the bureau's POA&Ms. **Exception Noted.**

- TTB - The evaluation team noted that weaknesses had been incorporated and prioritized. In addition, weaknesses identified in the security program review and assistance reports were documented in the POA&Ms. No Exception noted.

Summary: Based on the scope of this review, the evaluation team found that the Treasury POA&Ms did not always accurately reflect identified security weaknesses. In addition, weaknesses identified in the OIG reports did not always agree to the POA&Ms. Lastly, the evaluation team found that bureaus were inconsistently following the guidance from the OCIO and OMB for maintaining POA&Ms. Consequently, overall Treasury needs to work to improve the POA&M process.

Question 5 – OIG Assessment of the C&A Process

- The evaluation team inspected a total of 27 certification and accreditation packages, including documentation used to follow up on prior year certification and accreditation findings, as well as documentation used to determine the overall quality of the certification process used over the systems selected in the FY 2006 sample. All components of the certification and accreditation packages were inspected, including: the certification and accreditation methodology; risk assessment; system security plan; contingency plan; configuration management guide; incident response procedures; security awareness training; and security, testing and evaluation (ST&E) reports. Results of this review have been included below (the results for configuration management guide, incident response procedures, and security awareness training can be found under Questions 6, 7, and 8 respectively):

  - BEP – The evaluation team reviewed the certification and accreditation methodology used by BEP and noted that the methodology follows the guidance outlined in NIST Special Publication 800-37. The OIG chose the IBM 2066 eServer, MUTS, MFDT, PSMS, DATS, STS, and OST as the subset of systems from BEP to be reviewed as part of the FY 2006 FISMA assessment. The evaluation team reviewed the certification and accreditation documentation for each of these systems and noted that key elements required by NIST Special Publication 800-18, NIST Special Publication 800-30, NIST Special Publication 800-34, and NIST Special Publication 800-37 have not been included. Specifically, the evaluation team noted that key elements are missing from the IBM eServer system security plan, contingency plan, and risk assessment. The evaluation team

also noted that minor child systems have not been included in the system security plans of the BEP LAN/WAN and PSS system. Additionally, the evaluation team noted that a prior year finding with the Technical Security Division (TSD) Continuity of Operations Plan (COOP) has not been resolved. **Exception Noted.**

- BPD – The evaluation team reviewed the certification and accreditation methodology used by BPD and noted that the methodology follows the guidance outlined in NIST Special Publication 800-37. The evaluation team inspected the certification and accreditation documentation for the Bureau Automated Monitoring System (BATS), which was selected for review, and for the parent system, the Enterprise Information Technology Infrastructure (EITI). Following the inspection, the evaluation team determined that the BATS system has been identified in the certification and accreditation letter of EITI, the parent system. Additionally, the evaluation team noted that a prior year finding with the Oracle Federal Financials (OFF) system has been partially resolved. Specifically, the OFF risk assessment now addresses all of the requirements prescribed by NIST Special Publication 800-30, however several key elements required by NIST Special Publication 800-34 are still missing from the system's contingency plan. **Exceptions Noted.**

- CDFI –The evaluation team noted that the bureau has not taken steps to address a prior year finding related to the certification and accreditation process used for the CDFI LAN. Specifically, CDFI has not addressed several missing components in the contingency plan required by NIST Special Publication 800-34. Additionally, the CDFI certification and accreditation methodology does not state or display compliance with NIST Special Publication 800-37. **Exception Noted.**

- DO – The evaluation team reviewed the certification and accreditation methodology used by DO and noted that the methodology follows the guidance outlined in NIST Special Publication 800-37. The OIG choose the OCTS, TSAS, JAMES (child system of the FARS system), EEE, as well as Tracks FOIA Requests and Procedures reports, CFD, CCD, Library Acquisitions (eSubscriptions), and TECHLIB (all children of the DO LAN), as the subset of systems from DO to be reviewed as part of the FY 2006 FISMA assessment. First, the evaluation team noted that Treasury Headquarters Continuity of Operations Plan (COOP) and the system security plan created for EEE were missing several key elements required by NIST Special Publication 800-18, NIST Special Publication 800-34, and NIST Special Publication 800-37. Additionally, the evaluation team noted weaknesses in the certification and accreditation for FARS. Specifically, a signed copy of the certification and accreditation letter for FARS could not be provided as evidence that the system had been officially certified to operate. Additionally, the FARS child system JAMES was not identified within the letter. In addition, the evaluation team discovered that the OCTS and TSAS have not been certified and accredited. Lastly, child systems are not identified in the certification and accreditation documentation and security plan reviewed for the DO LAN. Specifically, for the Tracks FOIA Request and Procedures Report system, CFD, CCB, Library Acquisitions, and TECHLIB. Lastly the evaluation team noted that the DO has not taken steps to address a prior year finding related to the certification and accreditation process used for TACT. Specifically, DO has not addressed several missing components in the DO LAN System Security Authorization Agreement, which covers TACT. Additionally, the evaluation team was informed that the DO Headquarters COOP will cover TACT in the event of an emergency, however no mention of the system has been included in the plan. **Exception Noted.**

- FinCEN – The evaluation team noted that the bureau has not taken steps to address a prior year finding related to the certification and accreditation process used for the Information Technology Infrastructure (ITI). Specifically, FinCEN has not addressed several missing components in the risk assessment. Additionally, FinCEN has not finalized the ITI security plan and contingency plan. **Exception Noted.**

- FMS – The evaluation team reviewed the certification and accreditation methodology used by FMS and noted that it follows the guidance outlined in NIST Special Publication 800-37 for certifying systems to operate. The OIG choose ASAP, TOP, and ECP as the subset of systems from FMS to be reviewed as part of the FY 2006 FISMA assessment. Following a review of the certification and accreditation documentation for these systems, the evaluation team noted that several key elements required by NIST Special Publication 800-34 and NIST Special Publication 800-37 are not included in the contingency planning documentation. All other documentation generated to certify and accredit these systems appears to be in compliance with Departmental level and federal guidance. Lastly, a prior year finding relating to the FCAS Contingency Plan has not been addressed. Specifically, several elements required by NIST Special Publication 800-34 are missing from the plan. **Exception Noted.**

- Mint – The evaluation team reviewed the certification and accreditation used by the U.S. Mint and noted that the bureau follows the guidance outlined in NIST Special Publication 800-37 for certifying systems to operate. The OIG chose the Philadelphia –GSS/LAN (PH-LAN) and the Blackberry Service server as the subset of bureau systems to be reviewed during the FY 2006 FISMA assessment. The evaluation team noted that several key elements required by NIST Special Publication 800-18, NIST Special Publication 800-34, and NIST Special Publication 800-37 are missing from the system security plan and contingency plan of the PH-LAN. Additionally for the Blackberry Service server, which is a child system of the DC-LAN, the evaluation team noted that the system has not been identified in the certification and accreditation letter of the parent system. Lastly, the evaluation team noted that the bureau has not taken steps to completely address a prior year finding related to the certification and accreditation process used for the Documentum system. Specifically, the contingency plan for this system has been finalized, however it is out of date. The plan is currently being updated and revised to reflect the current operating environment. **Exception Noted.**

- OCC – The 401(k) Enrollment System and Training Administration System (children of the Workforce Operations system); the Appeals Tracking system (child of the Ombudsman system); the Examiner/e-File system, IT Provider Data Mart system, and the Shared National Credit Reporting System (children of the Examinations system); and Management and Accountability Reporting Tools system (child of the Fiscal Management system) were chosen to be the subset of OCC systems to be reviewed. Following an inspection of the certification and accreditation documentation for each of these systems, the evaluation team noted that several key pieces were missing or not properly documented for each system chosen. Specifically, the evaluation team inspected the certification and accreditation letters for the Examinations, Fiscal Management, Workforce Operations, and Ombudsman systems and noted that the child systems chosen as part of our subset of systems has not been identified in the documentation. In addition, the evaluation team inspected the system security plan for the Examinations system and Ombudsman system and noted the children system selected in our subset have not been included. However, the evaluation team determined that OCC management has developed a certification and accreditation methodology in accordance with NIST Special Publication 800-37. Finally, the

evaluation team followed up on a prior year finding regarding weaknesses in the Risk Analysis certification and accreditation documentation. Specifically, the evaluation team noted that several key elements required by NIST Special Publication 800-30, Special Publication 800-34 and Special Publication 800-18 are missing from the system's risk assessment, contingency plan and security plan, respectively. Also, the Risk Analysis system has not been identified in the OCC IT Disaster Recovery Plan. **Exceptions Noted.**

- OTS – The evaluation team noted that the bureau's certification and accreditation methodology is currently in draft. Additionally, the bureau has not taken steps to address the weaknesses in the ADM200 Personnel/Payroll system contingency plan. Specifically, several components required by NIST Special Publication 800-34 were not addressed. Lastly, a Security Test and Evaluation (ST&E) has not been performed for the ADM200 Personnel/Payroll system. **Exception Noted.**

- TIGTA – The evaluation team reviewed the certification and accreditation package for TMWI to determine if a condition identified during the FY 2005 FISMA assessment has been resolved. Following the review of this documentation, we concluded that the prior year condition with the TMWI risk assessment and contingency plan have not been resolved. Specifically, both documents still do not address all requirements of NIST Special Publication 800-30 and Special Publication 800-34 respectively. **Exception Noted.**

- TTB – As part of the FY 2006 FISMA review, the evaluation team selected the Integrated Revenue Information System (IRIS) for further review. Following an inspection of the certification and accreditation package of this system, the evaluation team discovered that the system was not identified in the certification and accreditation letter of the parent system, the Tax major application. **Exception Noted.**

Summary: The evaluation team reviewed 27 certification and accreditation packages and noted that all needed improvements. Treasury should work to improve the certification and accreditation process and enforce the use of NIST guidance when developing certification and accreditation documentation.

Question 6 – Configuration Management

- The evaluation team inspected data submitted by the bureaus regarding configuration management. The evaluation team assessed whether configuration guides were documented, and also determined whether an agency configuration management policy existed. Additionally, the evaluation team reviewed data supporting the implementation of the security configuration policy on the applicable systems as well as the process used to calculate the implementation percentage of a configuration guide.

  - Overall, the OCIO has developed and released the Treasury Information Technology Security Program. Volume 1 Part 1 of this document serves as the Department-wide security configuration policy, establishing a minimum baseline to be followed by all Treasury bureaus. Additionally, this document instructs and requires all bureaus to prepare configuration plans for all IT systems and networks. It also requires configuration and change management controls for the enforcement of the policy. The evaluation team noted that the guidance established in this document is consistent with the guidance in NIST Special Publication 800-53. No exceptions noted.

- The evaluation team noted that six out of eleven bureaus have developed overall configuration management policies; however these policies do not identify the specific platforms in use at the respective bureau and reference the configuration guides developed for each operating system and/or platform in use. Only BEP and TTB have documented the specific operating systems and/or platforms in use either within the Configuration Policy or supporting documentation. BPD, FinCEN, and OCC have configuration management policies in draft. **Exception Noted.**

- BEP – The evaluation team inspected the BEP Configuration Control Board Document and noted that it is in compliance with the guidance outlined by the OCIO above. Additionally, the evaluation team also discovered that BEP currently uses standardized software configurations on all platforms and performs continuous scanning of select systems to ensure compliance with established configuration guidelines. During the FY 2005 FISMA evaluation, the evaluation team determined that a configuration guide had not been developed for the Access Control Alarm Monitoring System (ACAMS). As part of the FY 2006 FISMA evaluation, the evaluation team followed up with BEP and again determined that a configuration guide had not been developed for ACAMS. **Exception Noted.**

- BPD – The evaluation team inspected the BPD configuration policy and determined that several key elements as required by the NIST Special Publication 800-53 were not identified. However, the evaluation team noted that BPD has established individual configuration guides for all platforms in use. **Exception Noted.**

- CDFI – The evaluation team inspected the CDFI Configuration Management Policy and noted that it is in compliance with the guidance outlined by the OCIO above. Additionally, the evaluation team noted that CDFI has created individual configuration guides for all platforms in use. Lastly, the evaluation team noted that a process has not been established for the calculation of the implementation percentage of a configuration guide. **Exception Noted.**

- DO – During the FY 2006 FISMA assessment, the evaluation team met with DO management to gain an understanding of the configuration management process and procedures used by DO. The evaluation team determined that DO has established an overall configuration policy for the bureau that sets guidelines for the development of platform-level configuration guides. However, the evaluation team determined that configuration guides are not available for various Microsoft Windows platforms, including Windows NT, Windows 2000 Professional, and Windows XP Professional. Additionally, the evaluation team also determined that DO does not have a sufficient process in place to determine the implementation percentage of a configuration guide. **Exception Noted.**

- FinCEN – The evaluation team determined that FinCEN is currently in the process of developing the Certification and Accreditation Services Configuration Management Guidelines. At the time of our assessment, this document was in draft. The evaluation team also reviewed configuration guides for Microsoft Windows 2000 Server, Windows 2003 Server, Windows XP Professional, and Sun Solaris and noted no exceptions. The evaluation team noted that FinCEN uses National Security Agency (NSA) and Defense Information Systems Agency (DISA) guides for configuration guides of Cisco IOS or Microsoft Windows 2000 Professional. To determine the implementation percentage of a configuration guide, FinCEN uses a standardized configuration on all new servers. Continuous scanning is also performed to ensure compliance throughout the life cycle of a system. **Exceptions Noted.**

- FMS – The evaluation team determined that FMS has documented configuration management procedures, as well as configuration guidelines, for all platforms in use. In addition, the evaluation team discovered that FMS has created a process for accurately determining the implementation percentage of a system configuration guide. No exceptions noted.

- Mint – The evaluation team determined that the U.S. Mint has developed an overall bureau level configuration management policy in accordance with the guidance outlined in the Treasury Information Technology Security Program Volume 1 Part 1. However, the bureau has not developed configuration guides for Microsoft Windows 2000 Professional, Windows NT, and the Macintosh Operating System. Individual configuration guides for all other platforms have been developed and implemented. To determine the implementation percentage of a configuration guide, the U.S. Mint uses a standardized configuration or image on all new servers. All devices are then scanned to ensure compliance with the original configuration; however these devices are not scanned periodically throughout their lifespan. Additionally, the Mint performs an inventory to determine the total number of systems. **Exceptions Noted.**

- OCC – The evaluation team determined that OCC is currently in the process of developing the Configuration Release Management Policy. However, at the time of our assessment, this document was in draft. The evaluation team was also not able to obtain configuration guides for Microsoft Windows NT, Windows 2000 Professional, IBM zOS, Cisco IOS, Sun Solaris, and Linux, all platforms currently operated by OCC. Lastly, the evaluation team discovered that OCC appears to not have developed a process for accurately computing the implementation percentage of a configuration guide. Specifically, OCC personnel were unable to clearly relay the process used for computing the implementation percentage of a configuration guide. **Exceptions Noted.**

- OTS – The evaluation team determined that OTS has developed an overall bureau level configuration management policy in accordance with the guidance outlined in the Treasury Information Technology Security Program Volume 1 Part 1. However, the evaluation team also noted that configuration guides are in place for all platforms, except for Microsoft Windows NT and Windows 2000 Server. Lastly, the evaluation team noted that OTS does have a process in place for determining the implementation percentage of a configuration guide. OTS has created standardized configurations and system configuration images, which are verified over the life of the system. **Exceptions Noted.**

- TIGTA – The evaluation team determined that TIGTA is currently in the process of developing a configuration management policy. However, at the time of our assessment, the document was still in draft. Additionally, the evaluation team discovered that TIGTA has created a process for accurately determining the implementation percentage of a system configuration guide. **Exception Noted.**

- TTB – The evaluation team inspected the TTB Information Technology Configuration Handbook and noted that it is in compliance with guidance outlined by the OCIO. The evaluation team also noted that TTB has created configuration guides for all platforms in use and has created a process to ensure compliance with these guides is monitored. This process includes the use of a standard image or security baseline for all new devices, and continuous scanning to ensure compliance. No exceptions noted.

Summary: The evaluation team noted that improvements are needed for the configuration management process. Specifically, configuration guides need to be developed for each operating system and an approved process should be used to support the implementation percentage for each security configuration policy.

Question 7 – Incident Detection and Handling Procedures

- The evaluation team inspected bureau and Treasury-wide incident response procedures and determined that the bureaus were responsible for reporting incidents internally to the Treasury Computer Security Incident Response Center (TCSIRC), and that Treasury is responsible for reporting incidents externally. Finally, the evaluation team inspected bureau monthly incident response reports submitted to TCSIRC to assess whether the bureaus followed the incident response procedures. The evaluation team inspected monthly incident response reports for all bureaus, with the exception of CDFI, and noted that the following information was captured on each report: misuse of resources, loss or theft of equipment with unclassified information, probes and reconnaissance scans, unsuccessful access or penetration attempts and malicious code detections. No exception noted.

- The evaluation team also inspected the Computer Security Incident Response Capability (CSIRC) procedures developed by each bureau for compliance with guidance outlined by the Department, as well as in NIST Special Publication 800-61. Only BEP, BPD, CDFI, FMS, and OCC have documented their bureau CSIRC procedures in accordance with Department-level guidance and NIST Special Publication 800-61. The documentation developed and implemented by the remaining bureaus is missing key required elements.

- The evaluation team also inspected monthly incident reports submitted to the TCSIRC to determine if policies and procedures were being followed for reporting incidents internally. Only CDFI and DO (HQ IT) did not submit all monthly incident reports to the TCSIRC during the period of review.

Summary: The evaluation team reviewed bureau and Treasury wide incident response procedures and determined that all but two (2) bureaus were following the guidance outlined by the OCIO. However, improvements are still needed to ensure that the incident response procedures have been documented in accordance with NIST guidance.

Question 8 – Security Training and Awareness

- The evaluation team inspected the Treasury IT security awareness training program for each bureau, and also inspected FY 2006 listings of employees and contractors who had completed the training. Additionally, the evaluation team judgmentally selected 30 individuals each from all 11 bureaus that had completed the IT security awareness training, and requested evidence that the training had been completed. Additionally, the evaluation team inspected evidence that the CIO, Deputy CIO, CISO, and other individuals received specialized training during the FISMA year. Results of this review follow:

    - TTB, BEP, BPD, CDFI, FMS, OTS, OCC and TIGTA – No exceptions were noted upon inspection of each bureau's IT security awareness training program.

- DO – The evaluation team inspected security awareness training documentation and noted that approximately 81% of DO's employees and contractors have completed security awareness training in FY 2006. No other weaknesses were noted regarding DO's IT security awareness training program. **Exception Noted.**

- FinCEN – The evaluation team inspected security awareness training documentation and noted that approximately 5% of FinCEN's employees and contractors have not completed security awareness training in FY 2006. Additionally, the evaluation team noted that one person did not attend specialized training during FY 2006. **Exceptions Noted.**

- Mint – The evaluation team inspected security awareness training documentation and noted that approximately 100% of the U.S. Mint's employees and contractors have completed security awareness training in FY 2006. However, the evaluation team verified that approximately 8% of the U.S. Mint's employees and contractors with significant security responsibilities have not received appropriate specialized training. **Exceptions Noted.**

Summary: Based on the scope of the review, the evaluation team determined that additional enhancements to the IT security awareness training program are needed at several bureaus. These bureaus and the OCIO should work to improve the IT security awareness training program by enforcing specialized training for personnel with significant security responsibilities, and by ensuring that all employees and contractors receive the annual security awareness training.

Question 9 – Peer-to-Peer File Sharing

- The evaluation team inspected documentation to assess whether bureaus addressed peer-to-peer file sharing in their IT security awareness training, ethics training, or any other agency wide training. The evaluation team also assessed whether employees and contractors received the training. Results of this review follow:

  - TTB, BEP, BPD, CDFI, DO, FinCEN, FMS, Mint, OCC, OTS, and TIGTA are addressing peer-to-peer file sharing in their IT security awareness training, ethics training, and other agency-wide training programs, as well as in various established policies. No exceptions noted.

Summary: Based on the scope of the review, the evaluation team determined that improvements have been made to the annual security awareness training at each bureau by including information on peer-to-peer file sharing in accordance with NIST Special Publication 800-16 and OMB M-06-20.

ATTACHMENT 2

Treasury Inspector General for Tax Administration—Security Management Act Implementation for Fiscal Year 2006

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 19, 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE TREASURY INSPECTOR GENERAL

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2006

We are pleased to submit the Treasury Inspector General for Tax Administration's (TIGTA) Federal Information Security Management Act (FISMA)[1] report for Fiscal Year 2006. The attached excel spreadsheet presents our independent evaluation of the status of information technology security at the Internal Revenue Service (IRS). We based our evaluation on the Office of Management and Budget (OMB) reporting guidelines.

During the 2006 evaluation period[2], we also conducted 14 audits to evaluate the adequacy of information security in the IRS. We considered results from these audits when making our assessment. Attached is a list of these specific audits.

The IRS has made steady progress in complying with FISMA requirements since the enactment of the FISMA in 2002. During 2006, the IRS reassessed the security risks of each of its systems. We are now confident that the inventory is substantially complete and the risk categorizations for its systems are accurate. The IRS also made significant improvements in the security certification and accreditation process. A working group[3], with participation from all the IRS business units, continued its weekly meetings to plan and refine processes for FISMA compliance. The IRS also continued to work closely in seeking guidance and concurrence on FISMA issues with the TIGTA, and the

[1] Public Law No. 107-347, Title III, 116 Stat. 2946 (2002).
[2] The FISMA reporting period for the Department of the Treasury is July 2005 through June 2006.
[3] IRS Security Program Management Office Council.

Department of the Treasury Chief Information Officer to improve compliance with the National Institute of Standards and Technology (NIST)[4] and FISMA requirements.

To complete our review we evaluated a representative sample of 15 IRS information systems to determine whether they had been certified and accredited, and whether security controls had been tested within the last year. We reviewed 10 IRS information systems to evaluate the adequacy of the certification and accreditation process; and conducted separate tests to evaluate processes for Plans of Action and Milestones (POA&M), configuration management, incident reporting, awareness training, training for employees with significant security responsibilities, and ensuring privacy of sensitive information. Our evaluation of the IRS' 2006 performance against specific OMB security measures, as well as our audit work performed during the 2006 evaluation period, show that the IRS still needs to do more to adequately secure its systems and data. Provided in this document are security performance improvements as well as areas that require additional attention.

Systems Inventory An accurate systems inventory is one of the cornerstones of an effective security program. The IRS updates its inventory on an ongoing basis and reviews the system inventory monthly and annually for accuracy and completeness. In this year's FISMA evaluation, the IRS reported on its total inventory of 264 systems. In addition, during the 2006 review period, the Office of Mission Assurance and Security Services, in coordination with each of the business units, re-evaluated the risk of all 264 systems. The risk categorization forms the basis for selecting an appropriate set of security controls to protect the confidentiality, integrity and availability of systems and data. We are confident that the systems inventory is substantially complete and the risk categorizations for IRS systems are accurate.

Certification and Accreditation Office of Management and Budget guidelines for minimum security controls in Federal information systems require that all systems be certified and accredited every three years or when major system changes occur. In the IRS, the Chief, Mission Assurance and Security Services is the certifying authority for all systems. The Chief, Mission Assurance and Security Services must test[5] the security controls in the information system and provide the results to the business unit owners. Business unit owners must then evaluate the information and determine whether to accredit the system, thereby giving it an authority to operate. By accrediting the system, the business unit owner accepts responsibility for the security of the system and is fully accountable for any adverse impacts if security breaches occur.

The IRS reported that 95.5 percent of it systems had current certifications and accreditations in Fiscal Year 2006. From our review of a sample (15 systems), we reported 100 percent had current certifications and accreditations. We attribute the difference to the limited number of systems we reviewed in our sample.

[4] The NIST, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.

[5] In testing the security controls, the certification agent determines the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system.

In 2006, the IRS developed a repeatable, NIST-compliant process designed to ensure a thorough assessment of system risk and security from which the system owner can make an appropriate accreditation decision. The IRS used this approach to evaluate its systems inventory. During our review we noted, however, problems with the execution of this process. For example, we found that application-specific controls were sometimes erroneously described as common controls and, as a result, they were not tested.

We also found examples of controls that were accepted without adequate testing. For example, tests of the account management controls for a moderate risk system were based on interviews only. Appropriate testing procedures should have included examinations of organizational records, user accounts, and configuration settings. Additionally, the business units did not always track weaknesses identified during the certification process for remediation.

Continuous Monitoring The NIST Special Publication 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Systems, states that a critical aspect of the security certification and accreditation process is the post-accreditation period involving the oversight and monitoring of the information system's security controls. The NIST requires the testing of an appropriate set of security controls every year throughout the system life cycle but not necessarily to the same extent required for a certification.

In 2006, the IRS did not make progress in implementing annual testing requirements. From our sample of 15 systems, we determined that the RS met annual testing requirements on only 7 of 15 (46.6 percent) systems we reviewed because they were tested during the certification process. On those systems that were not certified during the year, self-assessments were conducted but were generally based on tests of the operating systems only. We recognize these tests are useful; however, by not testing application-specific controls, business units cannot be confident that the privacy of sensitive taxpayer information is adequately protected.

The Department of the Treasury's Chief Information Officer recognizes that all bureaus need to improve compliance with the NIST annual testing requirements and recently issued draft guidance on the subject. The IRS agrees that this is an area for improvement and plans to have an improved process in place in Fiscal Year 2007.

Tracking Corrective Actions All Federal agencies are required to use the POA&M process to prioritize, track, and resolve security weaknesses. The IRS has developed, implemented, and is currently managing a POA&M process; however, the process needs improvement to ensure that all weaknesses from audit reports and vulnerability scans are tracked in POA&Ms.

From 9 TIGTA security reports issued during the 2006 FISMA reporting period, we could locate POA&Ms addressing only 11 of 41 (26.8 percent) recommendations and 11 of 47 (23.4 percent) proposed corrective actions. Also, in September 2005, the TIGTA issued an audit report[6] in which we reported that problems identified during vulnerability

[6] 2005-20-143, The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made (Reference Number 2005-20-143) dated September 2005.

scans and penetration tests were not formally provided to the business units, and corrective actions were not documented in POA&Ms.

Security Configuration Policies The OMB requires that agencies have configuration guides in place for software to ensure consistent implementation across the agency. During 2006, the IRS provided configuration guides for all 8 types of operating system, database, and router software running on IRS systems.

The IRS provided test results that demonstrated implementation for configuration policies for 6 of the 8 software types on at least 81-95 percent of the systems running the software. However, it could not provide documentation of testing done to demonstrate the extent to which security configuration guides were implementation for the other 2 software products. These software products, if improperly configured, could make the IRS' network vulnerable to disruptions of service and thefts of sensitive information by hackers, employees, and contractors.

Incident Reporting Procedures The IRS' Computer Security Incident Response Center (CSIRC) in the Mission Assurance and Security Services organization provides assistance and guidance for incident handling across the IRS enterprise. The CSIRC defines a security incident as: "any adverse event whereby some aspect of computer security could be threatened".

The loss or theft of an IT asset, including laptop computers and other portable devices, is a type of incident that could result in unauthorized access to systems and information. The IRS' incident reporting procedures require reporting this type of incident to an employee's first-line manager immediately upon detection, who should then notify the CSIRC and the TIGTA.

For 2006, we believe the IRS has not complied with CSIRC incident reporting policies and procedures. Employees' managers did not follow procedures for reporting the loss or theft of laptops and other portable devices to the IRS and the TIGTA. In a separate, on-going audit[7], we found the CSIRC and the TIGTA were not notified of incidents involving lost or stolen computer devices (e.g., laptops, blackberries).

We recognize that incidents regarding lost or stolen portable devices are not the only type of incidents that require reporting to the CSIRC and the TIGTA. However, due to the significance of this type of incident and the risk of loss and misuse of personal information that these incidents pose, it appears the IRS is not in compliance with incident reporting policies and procedures.

Awareness Training The NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, states that an awareness training program is crucial for all users since it is the vehicle for disseminating information that users need to do their jobs. The IRS provided security awareness training to all of its employees, but did not ensure all of its contractors received security awareness training. The IRS records showed that 998 contractors received security awareness training. Based on the 2,323 contractors reported by the IRS for 2006, we

[7] TIGTA Audit Number 200620001, Protection of Sensitive Data on Electronic Media (report due in November 2006).

determined that 1,325 (57 percent) did not receive security awareness training. To ensure that all contractors receive security awareness training, further improvements are needed.

Training Employees with Key Security Responsibilities The OMB requires all employees with key security responsibilities be given security-related training at least annually. The IRS has improved its performance in this area in 2006 and now has a process in place for identifying employees with significant security responsibilities. The IRS has also implemented the Electronic Learning Management System to centrally track specialized security training provided. However, further improvements are needed to ensure that employees with significant security responsibilities receive sufficient security training.

The IRS reported that 2,447 of 2,476 (99 percent) employees with significant security responsibilities received specialized security training during the reporting period. Since the OMB and NIST have not provided minimum training requirements for employees with key security responsibilities, the IRS considered an employee trained if he/she received any training during the reporting period. We determined, however, that only 1712 (69 percent) employees received 8 hours or more of training (an amount we arbitrarily selected) during the entire reporting period. The Department of the Treasury has indicated they will provide more specific training requirements for the 2007 reporting period.

Training employees with key security responsibilities requires more emphasis. We have attributed several weaknesses in past audit reports to the lack of training provided to these employees. Without sufficient training, these weaknesses will continue.

Privacy Requirements In March 2006, the TIGTA completed field work on an audit[8] to determine whether the Office of Privacy has effective controls and procedures to ensure IRS computer systems and employees adhere to privacy regulations. We determined that the IRS did not comply with Section 208 of the E-Government Act[9] on privacy requirements. Specifically, the IRS needs to take further actions to conduct evaluations for all systems and applications which collect personal information, and to enhance its processes to better monitor compliance with privacy policy and procedures. Since completing the fieldwork on this audit, the IRS made several improvements to better comply with privacy regulations by conducting privacy impact assessments for most of their systems and applications and developing an agency-wide privacy training program. Corrective actions are in process to complete assessments for the remainder of its applications, provide job specific privacy training, and improve continuous monitoring capabilities.


TIGTA FISMA 2006 Template 091506


2006 TIGTA_IT Audits.doc (73 K...

[8] Draft Audit Report – The Monitoring of Privacy Over Taxpayer Data Is Improving Although Enhancements Can Be Made to Ensure Compliance with Privacy Requirements (Audit # 200620002).
[9] E-Government Act of 2002, Public Law No. 107-347, Sec. 208 (December 17, 2002).

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name:

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

2. For each part of this question, identify actual performance over the past fiscal year by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Internal Revenue Service	High	4	2	0	0	4	2	2	100.0%	0	0.0%	0	0.0%
	Moderate	180	9	6	1	186	10	10	100.0%	5	50.0%	3	30.0%
	Low	73	3	1	0	74	3	3	100.0%	2	66.7%	1	33.3%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**257**	**14**	**7**	**1**	**264**	**15**	**15**	**100.0%**	**7**	**46.7%**	**4**	**26.7%**
Agency Totals	**High**	**4**	**2**	**0**	**0**	**4**	**2**	**2**	100.0%	**0**	0.0%	**0**	0.0%

Moderate	**180**	**9**	**6**	**1**	**186**	**10**	**10**	100.0%	**5**	50.0%	**3**	30.0%
Low	**73**	**3**	**1**	**0**	**74**	**3**	**3**	100.0%	**2**	66.7%	**1**	33.3%
Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**	0.0%	**0**	0.0%	**0**	0.0%
Total	**257**	**14**	**7**	**1**	**264**	**15**	**15**	100.0%	**7**	46.7%	**4**	26.7%

Question 3

In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.

3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 and/or NIST 800-53 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. Response Categories: Rarely, for example, approximately 0-50% of the time Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time - -	- Sometimes, for example, approximately 51-70% of the time
3.b.1.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Response Categories: Approximately 0-50% complete Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete - -	Approximately 96-100% complete -
3.b.2.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.	Missing Agency Systems:

		Missing Contractor Systems:
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	Yes
Question 4		

Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.

For items 4a.-4.f, the response categories are as follows:

Rarely, for example, approximately 0-50% of the time
Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time
-
-

4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Frequently, for example, approximately 71-80% of the time

4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	- Frequently, for example, approximately 71-80% of the time
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% of the time
4.e.	OIG findings are incorporated into the POA&M process.	- Frequently, for example, approximately 71-80% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Almost Always, for example, approximately 96-100% of the time

Comments: Question 2.b. - The IRS reported 61 percent of its systems were tested and evaluated in 2006. The IRS considered systems that had been certified and accredited within the reporting period as having been tested and evaluated. Using the same criteria we are reporting that 46.7 percent (7 of the 15 systems we reviewed) were tested and evaluated. We attribute the difference to the limited number of systems we reviewed in our sample. We did note that the IRS completed self-assessments during the review period for the remaining 8 systems; however, we are not recognizing self-assessments as a method of testing and evaluation. As we reported for FISMA 2005, self-assessment performance levels for applications are often based on tests of the General Support Systems which are usually conducted by the office of the CIO. We recognize these tests are useful. However, application-specific controls have not yet been selected and tested for each application as part of annual testing requirements, and business units have not been adequately involved in the testing. The IRS expects to have annual testing procedures in place in 2007. In our 2005 FISMA assessment, we reported our concern that the IRS and State agencies do not use NIST guidelines, to monitor the security of Federal tax information provided to State agencies. We did not follow up on this concern during this 2006 as

Question 5

OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans .

	Assess the overall quality of the Department's certification and accreditation process. Response Categories: Excellent Good - Satisfactory - Poor - Failing - -	- Satisfactory

Comments: We reviewed a sample of 10 applications that were certified and accredited during 2006. The IRS made substantial improvements to the C&A process during the 2006 FISMA reporting period. They have implemented a repeatable, NIST-compliant process designed to ensure a thorough assessment of system risk and security from which the system owner can make an appropriate accreditation decision. While we recognize and commend the IRS on this significant progress, the process needs further improvement to support an assessment level exceeding satisfactory. As we reported in Question 2, the IRS has not implemented procedures to ensure the continuous monitoring of security controls, a key requirement of the C&A process. Such procedures would require system owners to select a subset of controls for each system they own, to be tested in the interim years when a system is not scheduled for certification. The selection of controls is a system owner decision and should consider risk as well as the degree to which a control might degrade between certification cycles. The IRS recognizes the need to improve compliance with continuous monitoring requirements and has committed to developing a process and guidelines to better implement this control during 2007. In addition, our review of the System Security Plans (SSP) showed application-specific controls that were sometimes erro

Section B: Inspector General. Question 6, 7, 8, and 9.

Agency Name:

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
	Comments:	

6.b. Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows 2000 Professional	N/A	No	
Windows 2000 Server	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows 2003 Server	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Solaris	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
HP-UX	N/A	No	
Linux	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Other. Specify:			

Comments: Our assessment differs from IRS' assessment for systems running Linux and Oracle software. For each of these, IRS reported an implementation rate of, "Mostly, or on approximately 81-95 percent of the systems running this software", while we rated the two as, "Rarely, or, on approximately 0-50 percent of the systems running this software". Our ratings reflect that IRS could not provide documentation of testing done to support the extent to which the security

Question 7

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	No
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	No
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes

Comments: Questions 7.a. & b. - The IRS has not followed policies and procedures for reporting incidents internally or to law enforcement authorities. The IRS responded that they have followed incident reporting policies and procedures. Our response is based on a separate, on-going audit, in which we found that incidents involving lost or stolen computer devices (e.g., laptops, blackberries) were not reported to the CSIRC or the TIGTA. Results are still being compiled and will be reported in a separate report. We recognize that incidents regarding lost or stolen portable devices are not the only type of incident required to be reported to the CSIRC and the TIGTA. However, due to the significance of this type of incident and the risk of loss and misuse of personal information that these incidents pose, it appears that the IRS is not in compliance with incident reporting policies and procedures.		
Question 8		
8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Sometimes, or approximately 51-70% of employees have sufficient training
Comments: We are supplementing this response with comments because a single response choice cannot be applied to the two separate performance measures addressed in Question 8; namely, awareness training for all employees (including contractors) as well as specialized security training for employees with significant security responsibilities. Awareness training - The IRS provided security awareness training to all of its employees, but did not ensure awareness training was provided to all contractors. The IRS records showed that 998 contractors received awareness training. Based on the 2,323 contractors reported by the IRS for 2006, we determined that 1,325 (57 percent) did not receive security awareness training. Further improvements are needed to ensure that all contractors receive awareness training. Specialized security training - we disagree with the IRS' response that 99 percent (2,447 of 2,476) of employees with significant security		
Question 9		
9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

TIGTA IT Security Reports Issued During the 2006 Evaluation Period

1. Security Controls for the Taxpayer Advocate Management Information System Could Be Improved (Reference Number 2005-20-100) dated July 2005
2. Managers and System Administrators Need to Limit Employees' Access to Computer Systems (Reference Number 2005-20-097) dated July 2005
3. More Management Attention is Needed to Protect Critical Assets (Reference Number 2005-20-108) dated July 2005
4. Security Controls Were Not Adequately Considered in the Development and Integration Phases of modernized Systems (Reference Number 2005-20-128) dated August 2005
5. Monitoring Prime Contractor Access to Networks and Data Needs to Be Improved (Reference Number 2005-20-185) dated September 2005
6. Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected (Reference Number 2005-20-184) dated September 2005
7. Internal Penetration Test of the Internal Revenue Service's Networked Computer Systems (Reference Number 2005-20-144) dated September 2005
8. The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made (Reference Number 2005-20-143) dated September 2005
9. Contracting for Information Technology Goods and Service Generally Provided Intended Benefits; However, Maintenance Contracts Were Not always Supported (Reference Number 2005-20-187) dated September 2005
10. Federal Information Security Management Act Report for Fiscal Year 2005 (Reference Number 2006-20-071) dated October 2005
11. Progress Has Been Made in Using the Tivoli Software Suite, Although Enhancements Are Needed to Better Distribute Software Updates and Reconcile Computer Inventories (Reference Number 2006-20-021) dated December 2005
12. Secure Configurations Are Initially Established on Employees Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation (Reference Number 2006-20-031) dated February 2006
13. The Internal Revenue Service Successfully Accounted for Employees and Restored Computer Operations After Hurricanes Katrina and Rita (Reference Number 2006-20-068) dated March 2006
14. The Enterprise-Wide Implementation of Active Directory Needs Increased Oversight (Reference Number 2006-20-080) dated May 2006

ATTACHMENT 3

INFORMATION TECHNOLOGY: Fiscal Year 2006 Evaluation of Treasury's FISMA Implementation for Its Non-Intelligence National Security Systems [LIMITED OFFICIAL USE]

*** ***PROVIDED SEPARATELY*** ***

ATTACHMENT 4

INFORMATION TECHNOLOGY: Additional Actions Needed for System Inventory

*** ***PROVIDED SEPARATELY*** ***